

HUNTON & WILLIAMS

1900 K STREET, N.W.

WASHINGTON, D.C. 20006-1109

TELEPHONE (202) 955-1500

FACSIMILE (202) 778-2201

MCLEAN, VIRGINIA
MIAMI, FLORIDA
NEW YORK, NEW YORK
NORFOLK, VIRGINIA
RALEIGH, NORTH CAROLINA
RICHMOND, VIRGINIA
WARSAW, POLAND

SCOTT D. BALDERSTON
E-MAIL: SBALDERSTON@HUNTON.COM

FILE NO.: 55789,000003
DIRECT DIAL: (202) 955-1935

April 20, 2000

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Filing of New U.S. Patent Application Based on
Provisional Application *Serial No. 60/131,904*
Title: *SYSTEM AND METHOD FOR NETWORK SECURITY*
Inventors: John D. Abromavage, Mark Longworth, Todd A. Moore,
Scott V. Totman and Vince Romano
Attorney Docket No.: 55789,000003

Dear Sir:

Attached is a new patent application for filing in the United States Patent and Trademark Office including (18) pages of Specification, (7) pages of Claims (numbered 1-54), (1) page Abstract, (4) sheets of Drawings, and an executed Joint Declaration. This application claims priority to U.S. Provisional Application Serial No. 60/131,904 filed April 30, 1999.

The filing fee is calculated as follows:

		BASIC FILING FEE		AMOUNT
No. of Claims		No. in Excess	Rate	\$690.00
Number of Claims in Excess of: 20	54	34	\$ 18.00	612.00
Independent Claims in Excess of: 3	2	0	\$ 78.00	0.00
First Presentation of Multiple Dependent Claims			\$ 130.00	
Reduce by 1/2 for Small Entity				
TOTAL FEE DUE				\$1,302.00



09/552878 - 04/20/00

HUNTON & WILLIAMS

BOX PATENT APPLICATION

Page 2

A check in the amount of \$1,302.00 is attached to cover the basic application filing fee and additional claims fee. In the event of any variance between the amount enclosed and the Patent and Trademark Office charges, please charge or credit any difference to the undersigned's Deposit Account No. 50-0206.

Please direct all communication concerning this application to the undersigned as follows:

Scott D. Balderston, Esq.
Hunton & Williams
1900 K Street, N.W., Suite 1200
Washington, DC 20006
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Respectfully submitted,

HUNTON & WILLIAMS

By: Scott D. Balderston
Scott D. Balderston
Registration No. 35,436

Dated: April 20, 2000

03552678-042000

SYSTEM AND METHOD FOR NETWORK SECURITY

Field of the Invention

The invention relates to the field of communications, and more
5 particularly to advanced network security.

Background of the Invention

The consistent demand for computer and other network services has
increased the need for better network security tools. A variety of techniques
10 have been deployed to shield networks from hacking and other intrusions.
Those protective techniques may be categorized as either risk avoidance
systems or risk management systems.

Risk avoidance techniques involve introducing a barrier to prevent
inappropriate entry into a network. Such systems place reliance on keeping
15 intruders out of the network entirely, rather than monitoring inappropriate
network traffic after logging in. Risk avoidance systems include dedicated
network firewalls and mandatory encryption over the network. Commercial
examples include Gauntlet™, Firewall-1™, Guardian™, BorderWare™ and
others.

20 Risk management approaches, in contrast, adopt the philosophy that a
network can not keep everyone out, and so rely upon detection of intrusive
activity after logging in. Unfortunately, intrusion detector systems often lend a
false sense of security to systems administrators, while not really solving the

09552878-042000

underlying security problem. Intrusion detector systems produce a high rate of false positive identification, by inaccurately reporting legitimate network activity as suspicious. Intrusion detector systems also often overwhelm a systems administrator with too much detail about network behavior, and moreover are configured to trigger a report only after discovery of a network attack. Of course, at this point in time it is too late to prevent the attack or often to remedy much of the possible damage. Commercial examples include ISS RealSecure™, NetRanger™, TACAS+, NFR and others.

After-the-fact auditing systems provide another type of tool used under the risk management approach. Auditing systems are implemented as a host-based technique, in which a central server running the operating system logs the activity of client computers in a central storage area. However, the host computer running the audit system itself may be susceptible to being attacked internally or externally, creating a point of vulnerability in the overall surveillance.

Some other auditing products, such as Session Wall-3™ from AbirNet, employ so-called sniffer technology to monitor network traffic. Data streams collected by such products look for specific types of network traffic, for example, detecting electronic mail uploads by monitoring port 25 for simple mail transfer protocol (SMTP) events. However, most networks carry a large amount of traffic and sniffer type tools do not help sift through the volume. Other drawbacks exist.

captured and profiled and profiling is not dependent on one subset of port

The invention overcoming these and other pro

The collected information, typically in the form of packets, is subjected

assignments or boundary conditions, forensic inspection of past network activity is enhanced.

Brief Description of the Drawings

The invention will be described with respect to the accompanying
5 drawings, in which like elements are represented by like numbers.

Fig. 1 illustrates a network architecture for security according to the invention.

Fig. 2 is a flow chart illustrating surveillance and auditing processing according to the invention.

10 Fig. 3 illustrates a presentation interface for viewing and analyzing data collected by the invention.

Fig. 4 illustrates the operation of an interpreter module according to the invention.

Fig. 5 illustrates the operation of an assembler module and parser
15 module according to the invention.

Detailed Description of Preferred Embodiments

The invention will be described with respect to a network architecture illustrated in Fig. 1, in which a network observation port 104 monitors a
20 network data stream 144 traveling over a network 142. Network 142 may be or include as a segment any one or more of, for instance, the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide

09552873-042000

Area Network) or a MAN (Metropolitan Area Network), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3 or E1 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or FDDI (Fiber Distributed Data Networks) or CDDI (Copper Distributed Data Interface) connections.

10 Network 142 may furthermore be or include as a segment any one or more of a WAP (Wireless Application Protocol) link, a GPRS (General Packet Radio Service) link, a GSM (Global System for Mobile Communication) link, a CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access) link such as a cellular phone channel, a GPS (Global Positioning System) link, a Bluetooth radio link, or an IEEE 802.11-based radio frequency link. Network 142 may yet further be or include as a segment any one or more of an RS-232 serial connection, IEEE-1394 (Firewire) connections, an IrDA (infrared) port, a SCSI (Small Computer Serial Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog
15
20 interfaces or connections.

The network data stream 144 traversing the network 142 in the illustrative embodiment is a sequence of digital bits, which network observation

09552878-042000

port 104 senses and collects. Network observation port 104 may be implemented in a computer workstation configured with a network interface card (NIC), with that device configured to promiscuous mode so that all data is communicated transparently through the network observation port 104.

5 However, in the implementation of the invention, network observation port 104 is preferably embedded in the network without a separate network address, so that its presence on the network is not discernible to network users. Network observation port 104 is likewise preferably installed on a network node, such as a computer workstation or server, which is not responsible for and
10 does not run the network operating system for the network 142. The computer workstation or server which hosts network observation port 104 may be, for instance, a workstation running the Microsoft WindowsTM NTTM, Unix, Linux, Xenix, SolarisTM, OS/2TM, BeOSTM, Mach, OpenStepTM or other operating system or platform software.

15 As the realtime network data stream 144 is sensed and collected, the network observation port 104 transmits a copy of the network data stream 144 in the form of collected data stream 106 to interpreter module 108 over connection 146. Interpreter module 108 accepts the collected data stream 106 and interprets the collected data stream 106 into logical groupings, as illustrated
20 in Fig. 4. This process is sometimes called fragment reassembly.

 For instance, interpreter module 108 may interpret collected data stream 106 into Ethernet packets in an Ethernet implementation, and strip information

00552878-042000

off from those packets that will be extraneous to the further treatment of the collected data stream 106.

In an Ethernet environment, address information in the header reflects a media access control (MAC) hardware address, which is an absolute value and not readily mapped to a user or host, which have a logical rather than physical address. The interpreter module 108 thus removes the portions of the collected data stream 106 which contain the hardware-bound Ethernet header and processes the IP packet content. Interpreter module 108 transmits the resulting data packets 110 over communications link 148 to an assembler module 112.

The assembler module 112 accepts the incoming data packets 110 to perform a next level of data analysis. More particularly, the assembler module 112 consolidates the arriving data packets 110 into complete session files 118 representing discrete network events, such as data access and downloads by individual users. Individual session files 118 may be, for instance, transfer control protocol (TCP) sessions reflecting Internet activity.

As another variety of detectable transmissions, streaming video connections may be transmitted using the user datagram protocol (UDP) standard which is a connectionless protocol, since individual packets do not relate to or depend on preceding or following packets. Given that a UDP packet arrives in data packets 110 and is unique, that packet is added to a reassembly queue 180 (illustrated in Fig. 1) by assembler module 112.

042002-0505

042002-0505

042002-0505

042025-2025

The parser module 120 stores an overall log of the sessions 140 into session database 122. Parser module 120 contains application sensor module 126 that is invoked for each session 140 to determine the type of application that generated the session. Application sensor 126 uses port assignments, lexical
5 information and other data related to sessions 140 to determine what type of extractor 128 to invoke to process given session 140. Application sensor 126 includes a library of classes of extractors 128 to call up to process sessions 140.

Application sensor 126 characterizes the application type of sessions 140 by analyzing a variety of information contained in and characterizing the
10 session 140. That information may include source and destination addresses, sequence numbers, source and destination ports, and other parameters as illustrated in Fig. 5.

Sessions 140 of TCP and other protocols are characterized based in part upon a keyword lexicon analysis. In this regard, parser module 120 contains a
15 lexicon module 174 which analyzes sessions 140 to flag the presence of keyword phrases consistent with different types of TCP sessions. Accumulated information concerning these flags, such as the presence of discreet keywords or totals for keyword occurrences, are used to identify enumerated network objects.

20 For some types of network information, the occurrence of a single keyword may indicate the presence of an associated data object. For others, the total number of keyword occurrences, a weighted metric or other information

09552873-042000

may be compared to a threshold or other criteria to establish that category of event.

For instance, the presence of the phrase “/r/nfrom:” is illustratively flagged for candidacy as both an email and news article object. However, the keyword “/r/nNewsGroup:” correlates only to a news object. The logical trigger for news articles may be the presence of a flag for “/r/nnewsgroup:” being present and flagged. Similarly, the logical trigger for the presence of email may be positive flags for the terms “/r/nFrom:” in addition to the phrase “/r/nTo:”.

An example of a procedure call, invoked by the sensor module 126, to identify an SMTP event follows. The code in the following table (illustratively in C++, although it will be understood that other languages may be used) may be employed according to the invention to isolate those types of mail transmissions.

Table 1

```
15      ^HELO {
          FlagIt (APP_STATE, APP_SMTP, SMTPHELO);
      }
20      ^data[S] {
          FlagIt (APP_STATE, APP_SMTP, SMTPDATA);
      }
      ^data\r {
          FlagIt (APP_STATE, APP_SMTP, SMTPDATA);
      }
25      ^"mail from"[ ]*: {
          FlagIt (APP_STATE, APP_SMTP, SMTPMAILFROM);
      }
      ^"rcpt to"[ ]*: {
30          FlagIt (APP_STATE, APP_SMTP, SMTPRCPTTO);
      }
```

```
^EHLO {  
    FlagIt (APP_STATE, APP_SMTP, SMTPHELO);  
}
```

```
5 #define MINSMTPMATCH(X) ((X) & SMTPHELO && (X) & SMTPDATA  
  && (X) & SMTPRCPTTO)
```

According to the foregoing procedure call, each occurrence of the word

10 "HELO" preceded by a line feed ('\n') is flagged as a SMTPHELO. According to the Minimum Match Criteria (MINSMTPMATCH), if a 'SMTPHELO', 'SMTPDATA', and 'SMTPRCPTTO' is found, the match is made and an SMTP parser is called.

15 Similarly, in terms of profiling and triggering a HTTP/HTML event, the following procedure call may be employed.

Table 2

```
20 "GET " { /*BEGINNING of HTTP STUFF */  
    FlagIt (APP_STATE, APP_HTTP, HTTPGET);  
}  
"Referer: " {  
    FlagIt (APP_STATE, APP_HTTP, HTTPREFERER);  
}  
25 "Accept: " {  
    FlagIt (APP_STATE, APP_HTTP, HTTPACCEPT);  
}  
"User-Agent: " {  
    FlagIt (APP_STATE, APP_HTTP, HTTPUSERAGENT);  
30 }  
"HTTP"/"[0-9]". "[0-9]" {  
    FlagIt (APP_STATE, APP_HTTP, HTTPVERSION);  
35 }  
/* HTML FLAGS */
```

000240-8-2925560

```
"<HTML" {  
    FlagIt (CONTENT_STATE, CNT_HTML, HTMLTAG);  
}  
5  "<A HREF" {  
    FlagIt (CONTENT_STATE, CNT_HTML, HTMLHREF);  
}  
    "<H1" {  
        FlagIt (CONTENT_STATE, CNT_HTML, HTMLH1);  
10  }  
    "</a" {  
        FlagIt (CONTENT_STATE, CNT_HTML, HTMLANCHOR);  
    }  
15  "<HEAD>" {  
    FlagIt (CONTENT_STATE, CNT_HTML, HTMLHEAD);  
    }  
    "<BODY" {  
20  FlagIt (CONTENT_STATE, CNT_HTML, HTMLBODY);  
    }  
#define MINHTTPMATCH(X) ((X) & HTTPVERSION)  
#define MINHTMLMATCH(X) ((X) & HTMLTAG && (X) & HTMLHEAD  
25  && (X) & HTMLBODY)
```

Other protocols may be triggered upon other corresponding lexical triggers, or other types of information when the network event is not textually-
30 based. For example, the original network data stream 144 may be sampled during a streaming video, voice-over-network or other virtual connections which are not encapsulated in a textual or TCP format.

Because network protocols may be nested, for example, a POP-3 session may contain one or more instances of RFC822 email sessions, application
35 sensor 126 may be applied recursively to identify protocols within other

protocols to extract nested or underlying objects encapsulated in one or more different protocols.

The protocols the invention may detect include, but are not limited to, TCP, IP, UDP, SMTP, HTTP, NNTP, FTP, TELNET, DNS, RIP, BGP, MAIL, NEWS, HTML, XML, PGP, S/MIME, POP, IMAP, V-CARD, ICMP, NetBUI, IPX and SPX objects, understood by persons skilled in the art. The universe of protocols that sensor module 128 can detect and identify is extensible, and can be added to or subtracted from to accommodate future protocols and for other network needs.

Once application type of session 140 has been determined by application sensor 126, parser module 120 may, depending upon configuration information and type of session, store part or all of a complete session to content database 182 after assignment of a unique storage address.

The parser module 120 also contains extractor module 128, which processes the determined protocol for a given session 140 and generates the minimum subset of information needed to identify the nature of session 140 for recording on session database 122, removing unnecessary information before storage. Information may be reduced using text compression and other techniques. Because network protocols are designed to nest, extractor 128 is applied recursively to process protocols within other protocols, as identified by sensor 126. Depending on the category of session 140, the data reduction from

the original network sessions to the metadata image of the session (each stored on session database 122) may be on the order of 100 to 1 or greater.

Depending on the size of network 142, the bandwidth of network data stream 144 and other factors, the storage requirements of session database 122 may be substantial. However, the storage requirement of the invention is commensurate with the comprehensive nature of the surveillance performed and affords system administrators the opportunity to perform more fully featured post hoc traffic analysis.

At the back end of the network apparatus of the invention, a presentation interface 138 (illustrated in more detail in Fig. 3) communicates via communication line 168 to a presentation server 136. The presentation server 136 may be a workstation or other device, such as a personal computer running the Microsoft WindowsTM 95, 98, NTTM, Unix, Linux, SolarisTM, OS/2TM, BeOSTM, MacOSTM or other operating system. The presentation interface 138 may be accessed by a systems administrator wishing to perform network investigation or maintenance, and may be connected to presentation server 136 for example via a common gateway interface (CGI) bin or other Web service interfaces.

The presentation server 136 is in turn connected via communications link 166 to a summary database 132, which is in turn connected via connection 164 to session database 122. The session database 122 and summary database 132 may in one regard be serviced by the same database engine, such as an

online analytic processing (OLAP) interface. Execution of scripts through an OLAP or other engine such as a relational database engine accessed by Standard Query Language (SQL) generates the summary database 132 from searches on the session database 122.

5 Presentation interface 138 allows a systems administrator to invoke a graphical or other menu of different inquiries into the past behavior of network 142. Those inquiries may include an investigation of Websites most frequently visited by users of the network, individual users exhibiting the highest rate of e-mail traffic including images of the e-mail messages themselves, nodal analyses
10 of different network addresses and their most frequent communicants, and other information recorded in the resulting databases.

The variety of forensic inquiries that may be formulated through presentation interface 138 is in part a function of the complete nature of the surveillance performed by the invention, and the storage of the results of those
15 interrogations in summary database 132 also allows further treatment by characterization module 134 communicating with summary database 132 over connection 172.

The characterization module 134 may store high-level, digested data indicating the overall behavior of network 142, such as peak traffic times,
20 distribution of utilized bandwidths across the network over time, general degree of user activity and other categories of characteristic data.

09552878-012000

Presentation interface 138 may overlay the graphical or other depiction of the network behavior with system policy constraints or goals, such as limits on Web access or e-mail traffic, to visually show how different facets of the network are complying or behaving. Presentation interface 138 may, if desired, be connected to a printer or other output device (not shown) to produce hard copy of the different varieties of reports prepared according to the invention.

Similarly, summary database 132 may include ports to other external applications to receive further collateral information concerning network behavior, such as employee lists, accounting records and other packages.

The overall processing flow of the invention is illustrated in Figure 2. In step 202, processing begins. In step 204, bits from the network data stream 144 are collected by network observation port 104 into collected data stream 106. In step 206, the collected data stream 106 is transmitted to interpreter module 108. In step 208, the interpreter module 108 resolves the collected data stream 106 into data packets 110. In step 210, the assembler module 112 accepts additional packets from any external application ports, if any are present.

In step 212, assembler module 112 assembles data packets 110 into individual sessions 140, storing new sessions in session file 118. In step 214, assembler module 112 transmits copies of the sessions 140 to parser module 120. In step 216, the parser module 120 invokes the sensor module 126 to assign a session type to individual sessions 140.

0552378.042000

In step 218, the extractor module 128 is invoked to extract the minimum essential session data to be reflected in summary database 132. In step 220, parsed session information is stored in session database 122. In step 222, the summary database 132 is generated by executing OLAP scripts or other search or query mechanisms against session database 122. In step 224, the presentation interface 138 is presented to a systems administrator or other user.

In step 226, a user inquiry is accepted, such as an interrogation from a systems administrator. In step 228, the user inquiry is input to the presentation server 136. In step 230, the presentation server 136 analyzes the query parameters and communicates with the summary database 132. In step 232, the characterization module 134 is executed. In step 234, the resulting graphical or other data are presented to the user via the presentation interface 138. In step 236, processing ends.

The foregoing description of the system and method of the invention is illustrative, and variations in configurations and implementation will be apparent to persons skilled in the art. For instance, while the interpreter module 108 has been illustrated as accepting input form a single network observation port 104, interpreter module 108 could accept samples of the network data stream 144 from multiple ports.

Similarly, while presentation interface 138 has been illustrated as an interactive module accepting analytic requests from a user, predetermined sets of reports can be executed by presentation server 136, summary database 132

and associated components in batch fashion. While certain functions have been described as being stored on and executed by individual modules, servers and other network elements, it will be appreciated that different aspects of the control and analysis of the invention maybe executed by different computers or
5 other devices, in distributed fashion. The scope of the invention is accordingly intended only to be limited by the following claims.

09552873.042000

Claims

What is claimed is:

1. A system for extracting information from network data, comprising:
an input interface connected to at least one source of network data; and
5 a network event sensor, communicating with the input interface, the
network event sensor applying at least a lexical engine to the network data to
identify at least one network event.
2. The system of claim 1, wherein the at least one source of network data
comprises an observation port connected to a network and continuously
10 capturing network data from the network.
3. The system of claim 2, wherein the observation port comprises a
network interface card.
4. The system of claim 3, wherein the network comprises at least one of an
Ethernet network, a token ring network, and a TCP/IP network.
- 15 5. The system of claim 3, wherein the network interface card is invisible to
the network.
6. The system of claim 1, wherein the at least one source of network data
comprises stored network data.
7. The system of claim 6, wherein the stored network data comprise at least
20 one of captured network files, Website mirrors, archives of Usenet files, and
archives of email files.

0952679.042000

8. The system of claim 1, further comprising an interpreter module, the interpreter module scanning the network data to generate logical groupings of the network data.

9. The system of claim 8, wherein the logical groupings comprise packets.

5 10. The system of claim 8, wherein the interpreter module removes low-level encoding information from the network data to generate the logical groupings.

11. The system of claim 10, wherein the low-level encoding information removed by the interpreter module comprises hardware addressing information.

10 12. The system of claim 8, further comprising an assembler module, communicating with the interpreter module, the assembler module scanning the logical groupings to generate at least one session object.

13. The system of claim 12, wherein the at least one session object comprises at least one session file.

15 14. The system of claim 12, wherein the assembler module scans the logical groupings by examining at least one of source address, destination address, sequence numbers, source port, and destination port to generate the at least one session object.

20 15. The system of claim 12, wherein the network event sensor applies the lexical engine to the at least one session object to identify the at least one network event as at least one of a predetermined set of event types.

09552878.042000

16. The system of claim 15, wherein the lexical engine detects the presence of at least one predefined keyword to identify the at least one of a predetermined set of event types.

17. The system of claim 16, wherein the predetermined set of event types
5 comprises at least one of TCP, IP, UDP, SMTP, HTTP, NNTP, FTP, TELNET, DNS, RIP, BGP, MAIL, NEWS, HTML, XML, PGP, S/MIME, POP, IMAP, V-CARD, ICMP, NetBUI, IPX and SPX.

18. The system of claim 16, wherein the lexical engine accumulates a total number of occurrences for the at least one predefined keyword to identify the
10 event type.

19. The system of claim 18, wherein the lexical engine applies a threshold to the number of occurrences to identify the event type.

20. The system of claim 12, wherein the network event sensor applies the lexical engine recursively to identify more than one event type contained in the
15 at least one session object.

21. The system of claim 15, further comprising an extractor module, the extractor module extracting the at least one network event from the at least one session object according to the at least one of a predetermined set of event types.

20 22. The system of claim 21, wherein the extractor module comprises a library of extractor types, each of the extractor types corresponding to at least one of the at least one of a predetermined set of event types.

00552878.042000

23. The system of claim 22, wherein the extractor module stores a minimum subset of the network data to reconstruct the at least one network event.

24. The system of claim 23, wherein the minimum subset of the network data is stored in a database.

5 25. The system of claim 24, further comprising a presentation module, communicating with the database, the presentation module querying the database for information related to the at least one network event.

26. The system of claim 1, wherein the network event sensor also applies a port detection engine to the network data to identify the at least one network
10 event.

27. The system of claim 1, wherein the at least one source of network data comprises a plurality of sources of network data.

28. A method for extracting information from network data, comprising the steps of:

15 a) receiving network data from at least one source of network data; and
b) applying at least a lexical engine to the network data to identify at least one network event.

29. The method of claim 28, wherein the at least one source of network data comprises an observation port connected to a network and continuously
20 capturing network data from the network.

30. The method of claim 29, wherein the observation port comprises a network interface card.

000240-8/0825560

31. The method of claim 30, wherein the network comprises at least one of an Ethernet network, a token ring network, and a TCP/IP network.
32. The method of claim 30, wherein the network interface card is invisible to the network.
- 5 33. The method of claim 28, wherein the at least one source of network data comprises stored network data.
34. The method of claim 33, wherein the stored network data comprise at least one of captured network files, Website mirrors, archives of Usenet files, and archives of email files.
- 10 35. The method of claim 28, further comprising a step of c) scanning the network data to generate logical groupings of the network data.
36. The method of claim 35, wherein the logical groupings comprise packets.
37. The method of claim 35, further comprising a step of d) removing low-
15 level encoding information from the network data to generate the logical groupings.
38. The method of claim 37, wherein the low-level encoding information comprises hardware addressing information.
39. The method of claim 35, further comprising a step of e) scanning the
20 logical groupings to generate at least one session object.
40. The method of claim 39, wherein the at least one session object comprises at least one session file.

09552878.042000

41. The method of claim 39, wherein the step (e) of scanning the logical groupings comprises a step of f) examining at least one of source address, destination address, sequence numbers, source port, and destination port to generate the at least one session object.

5 42. The method of claim 39, further comprising a step of g) identifying the at least one network event as at least one of a predetermined set of event types.

43. The method of claim 42, wherein the step (g) of identifying comprises a step of (h) detecting the presence of at least one predefined keyword to identify the at least one of a predetermined set of event types.

10 44. The method of claim 43, wherein the predetermined set of event types comprises at least one of TCP, IP, UDP, SMTP, HTTP, NNTP, FTP, TELNET, DNS, RIP, BGP, MAIL, NEWS, HTML, XML, PGP, S/MIME, POP, IMAP, V-CARD, ICMP, NetBUL, IPX and SPX.

45. The method of claim 43, wherein the step (h) of detecting comprises a
15 step of (i) accumulating a total number of occurrences for the at least one predefined keyword to identify the event type.

46. The method of claim 45, wherein the step (h) of detecting comprises a step (j) of applying a threshold to the number of occurrences to identify the event type.

20 47. The method of claim 39, wherein the step of b) applying at least the lexical engine comprises a step of k) applying the lexical engine recursively to identify more than one event type contained in the at least one session object.

0552878-042000

48. The method of claim 42, further comprising a step of l) extracting the at least one network event from the at least one session object according to the at least one of a predetermined set of event types.

49. The method of claim 48, wherein the step (l) of extracting comprises a
5 step of m) selecting at least one extractor module from a library of extractor types, each of the extractor types corresponding to at least one of the at least one of a predetermined set of event types.

50. The method of claim 49, further comprising a step of n) storing a minimum subset of the network data to reconstruct the at least one network
10 event.

51. The method of claim 50, wherein the step (n) of storing comprises a step o) of storing the minimum subset of the network data in a database.

52. The method of claim 51, further comprising a step of p) querying the database for information related to the at least one network event.

53. The method of claim 28, further comprising a step q) of applying a port
15 detection engine to the network data to identify the at least one network event.

54. The method of claim 28, wherein the at least one source of network data comprises a plurality of sources of network data.

Abstract

A system for network security transparently occupies an observation port on the data stream, passing the entire range of network information to a dedicated interpreter. The interpreter resolves the data stream into individual data packets, which are then assembled into reconstructed network sessions according to parameters such as protocol type, source and destination addresses, source and destination ports, sequence numbers and other variables. The different types of sessions may include the traffic of many different types of users, such as e-mail, streaming video, voice-over-Internet and others. The system detects and stores the sessions into a database. A parser module may extract only the minimum information needed to reconstruct individual sessions. A backend interface permits a systems administrator to interrogate the forensic record of the network for maintenance, security and other purposes. The invention is not constrained to detect limited types of data, but rather captures and records a comprehensive record of network behavior.

0965-2369

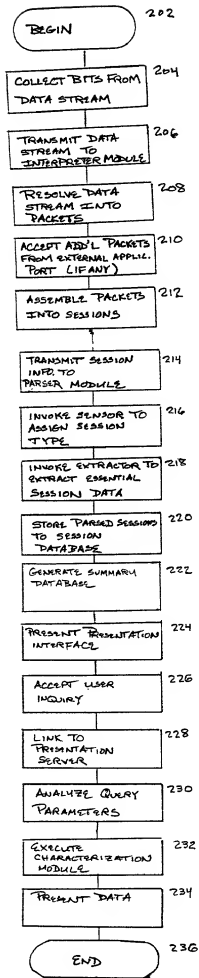


FIG 2

NefFor Analysis System - Microsoft Internet Explorer


http://38.180.230.245/docs_GW/index.html


Bookmark Help Export Status

 Search Target
 Any IP Search
 Any User Search
 Any Host Search
 Country Search
 Keyword Group Search
 Port Discovery

Target Analysis

 ANALYSIS REQUEST: User: E-Mail Sessions
 toddmoore

Date	From User	To User	Subject
Apr 9 1999 15:37	toddmoore@erols.com	Todd A Moore/CTX@ctx.com	mail test
Apr 9 1999 15:37	toddmoore@erols.com	Todd A Moore/CTX@ctx.com	mail test
Apr 9 1999 15:37	toddmoore@erols.com	todd a moore/ctx@ctx.com	mail test
Apr 9 1999 15:37	toddmoore@erols.com	todd a moore/ctx@ctx.com	mail test

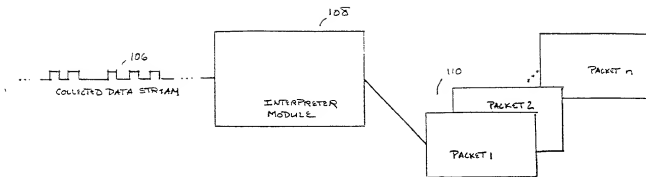


FIG. 4

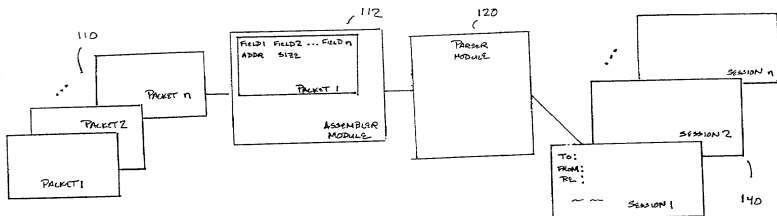


FIG. 5

09552878.042000

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residences, post office addresses and citizenship are as stated below next to our names:

We believe that we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled SYSTEM AND METHOD FOR NETWORK SECURITY, the specification of which

☒ is attached hereto.

☐ was filed on _____ as Application Serial Number _____ and was amended on _____

(if applicable)

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to in this declaration.

We acknowledge the duty to disclose all information known to us to be material to the patentability of this application, as defined in 37 C.F.R. § 1.56.

We acknowledge the duty to disclose to the Office all information known to us to be material to patentability as defined in § 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application Number	Date of Filing (day, month, year)	Date of Issue (day, month, year)	Priority Claimed Under 35 U.S.C. 119	
				Yes <input type="checkbox"/>	No <input type="checkbox"/>
				Yes <input type="checkbox"/>	No <input type="checkbox"/>
				Yes <input type="checkbox"/>	No <input type="checkbox"/>
				Yes <input type="checkbox"/>	No <input type="checkbox"/>

Prior United States Provisional Application(s)

I hereby claim the benefit under 37 C.F.R. § 119(e) of any United States provisional application(s) listed below

Application Number	Filing Date
60/131,904	30 April 1999

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

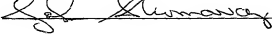
Application Serial Number	Date of Filing (day, month, year)	Status - Patented, Pending, Abandoned

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the following attorneys, their registration numbers being listed after their names:

Thomas J. Scott, Jr., Registration No. 27,836; James G. Gatto, Registration No. 32,694; Stanislaus Aksman, Registration No. 36,465; Henry C. Su, Registration No. 37,738; Christopher C. Campbell, Registration No. 37,291; Charles F. Hollis, Registration No. 40,650; Brian M. Buroker, Registration No. 39,125; Jonathan D. Link, Registration No. 41,548; Christopher J. Cuneo, Registration No. 42,450; Raphael A. Valencia, Registration No. 43,216; Kevin Duncan, Registration No. 41,495; Kevin J. Dunleavy, Registration No. 32,024; George Georgellis, Registration No. 43,632; Scott D. Balderston, Registration No. 35,436; Stephen T. Schreiner, Registration No. 43,097; Charles B. Lobsenz, Registration No. 37,857; Steven P. Klocinski, Registration No. 39,251; Yisun Song, Registration No. 44,487; Jennifer Albert, Registration No. 32,012; Carl Benson, Registration No. 38,378; Devin Morgan, Registration No. 45,562; Kerry Owens, Registration No. 37,412; Andrew Ririe, Registration No. 45,597; and Milan Vinnola, Registration No. 45,979.

All correspondence and telephone communications should be addressed to Hunton & Williams, 1900 K Street, N.W., Washington, D.C. 20006-1109, telephone number (202) 956-1500, which is also the address and telephone number of each of the above listed attorneys.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature  Date 4/19/00

Full Name of
First Inventor **ABROMAVAGE** **John** **D.**
Family Name First Given Name Second Given Name

Residence **13307 Jasper Road, Fairfax, VA 22033**

Citizenship **U.S.A.**

Post Office
Address **Same as above**

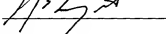
09552878.042000

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the following attorneys, their registration numbers being listed after their names:

Thomas J. Scott, Jr., Registration No. 27,836; James G. Gatto, Registration No. 32,694; Stanislaus Aksman, Registration No. 36,465; Henry C. Su, Registration No. 37,738; Christopher C. Campbell, Registration No. 37,291; Charles F. Hollis, Registration No. 40,650; Brian M. Buroker, Registration No. 39,125; Jonathan D. Link, Registration No. 41,548; Christopher J. Cuneo, Registration No. 42,450; Raphael A. Valencia, Registration No. 43,216; Kevin Duncan, Registration No. 41,495; Kevin J. Dunleavy, Registration No. 32,024; George Georgellis, Registration No. 43,632; Scott D. Balderston, Registration No. 35,436; Stephen T. Schreiner, Registration No. 43,097; Charles B. Lobsenz, Registration No. 37,857; Steven P. Klocinski, Registration No. 39,251; Yisun Song, Registration No. 44,487; Jennifer Albert, Registration No. 32,012; Carl Benson, Registration No. 38,378; Devin Morgan, Registration No. 45,562; Kerry Owens, Registration No. 37,412; Andrew Ririe, Registration No. 45,597; and Milan Vinnola, Registration No. 45,979.

All correspondence and telephone communications should be addressed to Hunton & Williams, 1900 K Street, N.W., Washington, D.C. 20006-1109, telephone number (202) 956-1500, which is also the address and telephone number of each of the above listed attorneys.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature  Date 19 APRIL 2000

Full Name of
Second Inventor **LONGWORTH** Mark
Family Name First Given Name Second Given Name

Residence **46642 Brownwood Square, Sterling, VA 20164**

Citizenship **U.S.A.**

Post Office
Address **Same as above**

00552878-0427000

Thomas J. Scott, Jr., Registration No. 27,836; James G. Gatto, Registration No. 32,694; Stanislaus Akseman, Registration No. 36,465; Henry C. Su, Registration No. 37,738; Christopher C. Campbell, Registration No. 37,291; Charles F. Hollis, Registration No. 40,650; Brian M. Buroker, Registration No. 39,125; Jonathan D. Link, Registration No. 41,548; Christopher J. Cuneo, Registration No. 42,450; Raphael A. Valencia, Registration No. 43,216; Kevin Duncan, Registration No. 41,495; Kevin J. Dunleavy, Registration No. 32,024; George Georgiellis, Registration No. 43,632; Scott D. Balderston, Registration No. 35,436; Stephen T. Schreiner, Registration No. 43,097; Charles B. Lobenz, Registration No. 37,857; Steven P. Klocinski, Registration No. 39,251; Yisun Song, Registration No. 44,487; Jennifer Albert, Registration No. 32,012; Carl Benson, Registration No. 39,738; Devin Morgan, Registration No. 45,562; Kerry Owens, Registration No. 37,412; Andrew Ririe, Registration No. 45,597; and Milan Vinicola, Registration No. 45,979.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Joe A. W. Moore

4/19/2000

Third Inventor

Family Name

First Given Name

Second Given Name

Address

Same as above

06-07-2019

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the following attorneys, their registration numbers being listed after their names:

Thomas J. Scott, Jr., Registration No. 27,836; James G. Getto, Registration No. 32,694; Stanislaus Aksman, Registration No. 36,465; Henry C. Su, Registration No. 37,738; Christopher C. Campbell, Registration No. 37,291; Charles F. Hollis, Registration No. 40,650; Brian M. Buroker, Registration No. 39,125; Jonathan D. Link, Registration No. 41,548; Christopher J. Cuneo, Registration No. 42,450; Raphael A. Valencia, Registration No. 43,216; Kevin Duncan, Registration No. 41,495; Kevin J. Dunleavy, Registration No. 32,024; George Georgellis, Registration No. 43,532; Scott D. Balderston, Registration No. 35,436; Stephen T. Schreiner, Registration No. 43,097; Charles B. Lobenz, Registration No. 37,857; Steven P. Klocinski, Registration No. 39,251; Yisun Song, Registration No. 44,487; Jennifer Albert, Registration No. 32,012; Carl Benson, Registration No. 38,378; Devin Morgan, Registration No. 45,562; Kerry Owens, Registration No. 37,412; Andrew Ririe, Registration No. 45,597; and Milan Vinnola, Registration No. 45,979.

All correspondence and telephone communications should be addressed to Hunton & Williams, 1900 K Street, N.W., Washington, D.C. 20006-1109, telephone number (202) 955-1500, which is also the address and telephone number of each of the above listed attorneys.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature

Scott V. Getto

Date

4/19/2000

Full Name of

Fourth Inventor

TOTMAN**Scott****V.**

Family Name

First Given Name

Second Given Name

Residence **302 Surveyors Court, Vienna, VA 22180**

Citizenship

U.S.A.

Post Office

Address

Same as above

0552878.042000

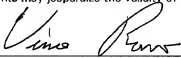
And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the following attorneys, their registration numbers being listed after their names:

Thomas J. Scott, Jr., Registration No. 27,836; James G. Gatto, Registration No. 32,694; Stanislaus Aksman, Registration No. 36,465; Henry C. Su, Registration No. 37,738; Christopher C. Campbell, Registration No. 37,291; Charles F. Hollis, Registration No. 40,650; Brian M. Buroker, Registration No. 39,125; Jonathan D. Link, Registration No. 41,548; Christopher J. Cuneo, Registration No. 42,450; Raphael A. Valencia, Registration No. 43,216; Kevin Duncan, Registration No. 41,495; Kevin J. Dunleavy, Registration No. 32,024; George Georgellis, Registration No. 43,632; Scott D. Balderston, Registration No. 35,436; Stephen T. Schreiner, Registration No. 43,097; Charles B. Lobsenz, Registration No. 37,857; Steven P. Klocinski, Registration No. 39,251; Yisun Song, Registration No. 44,487; Jennifer Albert, Registration No. 32,012; Carl Benson, Registration No. 38,378; Devin Morgan, Registration No. 45,562; Kerry Owens, Registration No. 37,412; Andrew Ririe, Registration No. 45,597; and Milan Vinnola, Registration No. 45,979.

All correspondence and telephone communications should be addressed to Hunton & Williams, 1900 K Street, N.W., Washington, D.C. 20006-1109, telephone number (202) 955-1500, which is also the address and telephone number of each of the above listed attorneys.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature



Date

4-19-00

Full Name of
Fifth Inventor

ROMANO
Family Name

Vince
First Given Name

Second Given Name

Residence **13140 Willaimsfield Drive, Ellicott City, MD 21042**

Citizenship **U.S.A.**

Post Office
Address **Same as above**

HUNTON & WILLIAMS

1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
Tel: (202) 955-1500

09552878-042000